



Release Notes

Illustra Flex 2MP 20X PTZ Dome

Firmware Version	Product Data
V2.01.01 (Illustra.SS002.01.01.00.1130)	Visit the IP Cameras section of our web site – www.illustracameras.com – to download datasheets and other documentation in PDF format.

December, 2017

Note:

In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

©2017 Tyco Security Products. All rights reserved.

8200-1307-09 B0

Table of Contents

Introduction	3
Previous firmware features	3
Firmware upgrade	4
New Features	5
Enhanced security	5
Automatic prompt for username and password change at first login	6
Login page and Session logout support	6
NVR integration on Enhanced security on firmware Illustra. SS002.01.01.00.1130	7
Special points and known limitations	8
Known issues	10
Contact information	12

Introduction

This document contains a summary of the key features and known limitations of firmware SS002.01.01.00.1130.

This firmware release applies the following cameras:

Camera Series	Model Number	Description
Illustra Flex	IFS02P5ICWTY	Illustra Flex 2MP 20x PTZ indoor, white,TDN, WDR
Illustra Flex	IFS02P5OCWTY	Illustra Flex 2MP 20x PTZ, outdoor, white, TDN, WDR

New features

- Fixed a Motion mask issue when integrating the Illustra Pro 12MP Fisheye with ExacqVision Server.

Previous firmware features

SS002.01.00.00.0620

- Enhanced security.
- Automatic prompt for username and password change at first login.
- Login page and session logout support.

SS002.01.00.00.0317

- No plugin requirements.
Web GUI no longer requires third party plugin (Quicktime, Java, Active X).
- DST (Day light saving) support.
When the time and date is set to either manual or NTP then the camera automatically applies daylight saving in time zones where this applies.

SS002.00.06.00.1128

- Initial release Firmware for product launch.

Firmware upgrade

WARNING: You can upgrade the camera firmware through the camera web browser interface, or through the Illustra Connect tool.

Note:

Upgrading the camera firmware does not affect existing camera settings.

Upgrade time for Flex PTZ Can take up to 10 minutes

Upgrading camera firmware using the web browser interface

To upgrade the camera firmware using the web browser interface, complete the following steps:

1. Using Internet Explorer, connect to the camera through the IP address and log in to the web browser interface.
 2. Select **Setup** on the web browser interface banner to access the setup menus.
 3. From the **System** menu, select **Maintenance**.
The Camera Upgrade tab is displayed.
 4. Select **Browse**.
The Choose file window is displayed.
 5. Navigate to where the firmware file is saved. Select the firmware file and then select the **Open** button.
 6. Select **Upload** to start the upgrade.
-

Upgrading the camera firmware using Illustra Connect

To upgrade the camera firmware using Illustra Connect, complete the following steps:

1. Install and launch the Illustra Connect software utility.
 2. From the displayed list of cameras; right-click on the camera that you want to upgrade.
 3. Select **Upgrade Firmware** to open the firmware upload window.
 4. Select **Choose File** and browse to the firmware upgrade file.
 5. Select **Upgrade** to start the upgrade.
-

Enhanced security

The enhanced security feature is intended to advance the security of the Illustra cameras by enforcing security best practices and adding features to help the installer and end users customize the camera's security to meet their controls.

The main changes include:

- A new security status page.
- Enforcement of complex passwords for all accounts, not just administrators.
- New behavior related to HTTP and video over HTTP.
- Updated auditing behavior (security logs).
- HTTP authentication methods: basic, digest.
- Force change of default username when in enhanced security mode.

Security Modes Summary

Standard Security

- Changes to communication protocols are available to all users with appropriate privileges.
- Password complexity is set to require a minimum of any 5 characters.
- Authentication method is set to basic by default.

Enhanced Security

- Unsecure protocols is disabled by default until enabled by a user.
- Discovery protocols is disabled by default until enabled by a user.
- Changes in the protocols is only available to a user with administrative privileges and require that user to reenter his/her password.
- Usernames for all accounts must meet the username password complexity requirements.
- Passwords for all accounts must meet the password complexity requirements.
- Authentication method is set to digest by default.

Username and Password complexity

Username as defined below:

- Minimum characters: 5

Password as defined below:

- Minimum characters: 7
- Cannot be identical to the username and must have one character from at least three of the following character groups:
 - upper case letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - lower case letters abcdefghijklmnopqrstuvwxyz
 - numeric characters 0123456789
 - special characters @ % + \ / ' ! # \$ ^ ? : , () { } [] ~ - _ `

Automatic prompt for username and password change at first login

The admin/admin user is hardcoded until a new admin username is created. The user is prompted at first boot/factory default to select either standard or enhanced.

For standard Security

A pop up is visible advising you to change your username and password.

- **A username & password change is recommended** – Note: the user can cancel out and continue with admin/admin.
- If the user sets a new username and password – admin/admin is automatically replaced.
- A password change is not supported in this window – this is managed via the user tab.

For Enhanced Security

A pop up is visible requiring you to change your username and password.

- **A username & password change is mandatory** – Note: If the user sets a new username and password – admin/admin is automatically replaced.
- Certain criteria apply to both the username and password (See [Username and Password complexity](#))
- The camera offers support to remove the default admin user manually.

To delete the default admin user account:

1. Create a new administrator user using admin/admin.
2. Logout of the existing user admin account.
3. Login to the new admin user account.
4. Delete the admin user account.
5. The new admin user is now the hardcoded admin user.

How to restore admin/admin:

1. Manually by adding admin/admin user.
2. Restore factory default camera.

Login page and Session logout support

The camera supports an opening login page with the Illustra logo. Localization selection is available on this login page. If the GUI is idle for some time, the camera returns to the login page, logging the user out for security purposes.

NVR integration on Enhanced security on firmware Illustra. SS002.01.01.00.1130

Flex PTZ Illustra.SS002.01.01.00.1130 with enhanced security features has some impact on the NVR integration.

The main change affecting the NVR integration is the introduction of RTSP authentication and the addition of HTTP Basic/Digest Authentication depending on the security option required.

Along with the firmware upgrade the end user requires a new iAPI3 handler for complete VENVR Integration.

Failure to update the handler results in no video to live stream or recording.

The new handler “default” security group automatically adjusts HTTP authentication by querying the camera directly – there is no need for the end user to create specific security groups.

From VE NVR 5.0 onward the iAPI3 handler upgrade is not required as the updated handler is directly merged to the core.

For ONVIF integration in 5.0 a security group requires configuration prior to the camera being added.

Special points and known limitations

WARNING: You can upgrade the camera firmware through the camera web browser interface, or through the Illustra Connect tool.

Due to the removal of the dependency on third party software the camera has the following features:

- Live video stream support across multiple browsers (IE9, IE10, IE11 Chrome, Firefox, and Safari).
- Live view stream using IPv6 address.
- Third party software, even if present, is no longer used.
- GUI live view always displays stream 3 MJPEG (see specific camera for resolution details).
- Privacy zone drawing is now supported on all browsers (IE9, IE10, IE11 Chrome, Firefox, and Safari).
- Motion detection Zone drawing now supported on all browsers (IE9, IE10, IE11 Chrome, Firefox, and Safari).
- The double login seen on previous firmware is resolved.
- GUI audio is no longer supported.

Special points and known limitations	Workaround
When in TrueWDR mode and OSD is enabled, flicker can occur in stream 2 and stream 3 when stream 2 and 3 are not using the same fps.	If OSD is required in TWDR mode, match stream 2 and Stream 3 fps to remove all flicker.
The camera supports UPnP discovery. However, this feature is always enabled and cannot be disabled.	By design.
The camera only supports edge metadata alert events. For more information, refer to the edge analytics support table.	N/A.
During the configuration of analytics, or when enabling or modifying motion detection rules, video streams are affected. When the change is applied, it causes video streams to restart causing a small loss of video. Video functionality is restored within seconds.	N/A.
Each backup configuration file is specific to the camera and firmware version. Therefore, if a camera is upgraded, the old backup file becomes obsolete and the camera needs to be updated with a new copy. For example, a backup file created on a camera running on 1.0 firmware cannot be installed on a camera running 2.0.	N/A.
The camera supports DHCP IP allocation for IPv4 addresses but does not support IPv6 IP ranges. IPv6 is only supported through linking local addresses.	N/A.

Flex PTZ analogue-out does not support the rotate feature. Analogue always shows the native stream as per the camera mount.	N/A
When a Flex PTZ preset saves the PTZ position with focus iris no picture setting edits are saved.	Future implementation

Known issues

Known issues	Workaround
When enabling video recording - S.D. recording, FTP, CIFS, and SMTP, if analytics are already configured and enabled, events are not recorded.	Enable analytics prior to configuring an event action. If analytics weren't enabled prior to configuring an event action, disable and re-enable analytics to start recording events.
When performing a factory reset through the camera web interface and you select the check box to retain IP settings, all user profiles are preserved rather than reset to default admin login.	To reset the user profile to the factory default, select Setup , select System , select Maintenance , select Reset , or alternatively, hold down the reset button for more than 20 seconds.
The IP video can be rotated in different directions. This is only supported on IP video and the duplicate rotation is not reflected on the Analogue-Out video output.	If using analogue video, rotate the lens to the desired orientation.
After a period of inactivity, an open web interface session can be slow to respond to a navigation request. Normal response is restored within a few seconds.	Avoid leaving the browser idle for long periods.
The camera can save a backup configuration file for future restorations. However, this feature is not supported when using the ONVIF integration.	Camera backup can be performed through the camera web interface.
The camera web interface can be configured to several languages. When the camera web user interface is configured to Arabic, some screen resolutions may display text that is too small to read.	If the Arabic text is difficult to read, use the browser window zoom utility to increase the text size.
<p>If using the ONVIF device manager to upgrade the units, the tool needs to be provided with camera authentication, in order for the upgrade to complete successfully.</p> <p>During the upgrade an error message can appear. The message is: Failed to read enough bytes on the stream. The upgrade completes successfully, regardless of the error message.</p>	Use the Illustra connect tool to upgrade the camera. This tool does not have the limitation and can also provide batch upgrades on units that are running the same firmware.
Camera events are cleared when the firmware is upgraded. This only affects logs. Recorded video on SD cards is not cleared when the firmware is upgraded.	N/A.
The date and time on the camera web browser interface offsets incorrectly during DST time changes. All other times	Resolved.

displayed on the web browser interface and the time registered internally maintain the current time. This relates to OSD time, event time, metadata event time, logs, and recorded clips time.	
On the Illustra Flex PTZ camera, presets are saved but don't retain manual focus. Auto focus will run once preset is reached.	None.
On the Illustra Flex PTZ camera, manual iris is not supported through IAPI3 operations and integrations.	Configure manual iris using the camera web user interface.
On the Illustra Flex PTZ camera, enabling automatic flip can cause the camera to move to the top end of the scene.	None.
Backup/Restore > The backup configuration file does not restore PTZ present pattern and sequences or privacy zones when restoring from file.	Restore privacy zone and PTZ features manually.
DDN username field does not allow for special character	Targeted for future implementation
Some sections of the initial login are not fully localized and shown in English.	Targeted for future implementation
When performing a factory reset through the camera web interface and you select the check box to retain IP settings, all user profiles are preserved rather than reset to default admin login.	Retain IP now only retains IP settings. User credentials are reset.
Navigating between GUI tabs that provide a Live view preview and those that don't may not always restore live stream (image paused) between pages.	Start the stream again by selecting the play button
Adding or removing privacy zones will trigger motion events if enabled.	Configure privacy zones prior to Enabling motion detection.
Event action setting (record, FTP, CIF,) do not verify if a SD card is inserted or not before allowing activation.	User shall manually check if SD card is inserted by navigating to the Edge recording tab.
CIFS will only support image transfer, no video will be transferred	If video is required to transfer please use FTP

Contact information

If you have any questions regarding these release notes, please contact Tyco Security Products Technical Services at:

Toll Free: 800-507-6268, Option 2 **International:** 561-912-6259, Option 2 **Alternative Number:** 800-392-2873
Fax: 450-444-2029 **Hours:** 08:00 – 20:00 EST
Email: adtechservices@tycoint.com **Website:** www.illustracameras.com

In Europe, Middle East and Africa, contact Technical Support at:

Toll Free: +800 CALLTYCO or +800-2255 8926 **Direct:** +31 475 352 722
Hours: 08:00 – 18:00 CET **Email:** : EMEA-Video-Support@tycoint.com
Website: www.tycosecurityproductsemea.com **Website:** www.calltyco.com

Local Direct dial numbers:

UK	08701 238 787	Bahrain	800 04127
France	0800 90 79 72	Greece	00800 31 229 453
Spain	900 99 39 61	Russia	810 800 20 521 031
Germany	0800 1806 757	Turkey	00800 31 923 007
Italy	0800 874 091	United Arab Emirates	800 0310 7123
Belgium	0800 76 452	Israel	03 345 6868
Ireland	021 480 1122		

In Latin America and Caribbean, contact Technical Support at:

Southern Latin America Contact: Cesar Cristal Phone: +54-11-4711-8711 Cell: +54911-6452-7573 Email: ccristal@tycoint.com	Brazil (North) Contact: Wagner Soares Phone: +55 (21) 2108-6016 x.250 Cell: +55 (21) 99153-3519 Email: wsoares@tycoint.com	Brazil (South) Contact: Dani Hissnauer Miguel Phone: +55 (11) 2172 9224 Cell: +55 (11) 97663-2653 Email: danimiguel@tycoint.com
Northern Latin America & Caribbean Contact: Hildebrando Duran Phone: +57-1638-6278 Cell: +57-317668-9590 Email: hiduran@tycoint.com	Mexico Contact: Marco Antonio Salguero Phone: +52-55-5488-8092 Cell: +52-55-1473-4946 Email: msalguero@tycoint.com	

In Asia Pacific, contact Technical Support at:

Toll Free: +800 CALLTYCO or +800-2255 8926 **Direct:** +86 21 60 23 0650
China Only Hotline: 400 671 1528 **India Only Hotline:** 1 800 1082 008
Hours: 08:00 – 17:00 CST **Email:** apac.support@tycoint.com

Information furnished by Tyco Security Products is believed to be accurate and reliable. However, no responsibility is assumed by Tyco Security Products for its use, nor any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent rights of Tyco Security Products.
